Logo

[] \*

**POPIS PRACOVNÍHO MÍSTA POVĚŘENCE PRO**

**OCHRANU OSOBNÍCH ÚDAJŮ**

|  |  |
| --- | --- |
| Označení: |  |
| Verze: |  |
| Datum verze: |  |
| Vytvořil: |  |
| Schválil: |  |
| Klasifikace: |  |

**Historie změn**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Verze** | **Vytvořil** | **Popis změny** |
| dd.mm.rrrr | 1.0 | ACRESIA Consulting | Vytvoření dokumentu |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Obsah**

[1. Účel, rozsah a uživatelé 3](#_Toc74731776)

[2. Účel pracovního místa 3](#_Toc74731777)

[3. Zařazení v organizační struktuře 3](#_Toc74731778)

[4. Vymezení odpovědností 3](#_Toc74731779)

[4.1. Základní úkoly 4](#_Toc74731784)

[4.2. Další možné pracovní úkoly 4](#_Toc74731785)

[5. Autorita 5](#_Toc74731786)

[6. Platnost a správa dokumentů 5](#_Toc74731787)

# Účel, rozsah a uživatelé

Pro dosažení souladu s ustanoveními obecného nařízení EU o ochraně osobních údajů GDPR a pro zajištění trvalého dodržování všech hlavních činností organizace [název organizace] (dále jen "organizace"), bylo rozhodnuto, že pracovní pozice pověřence pro ochranu osobních údajů bude vytvořena.

Pověřenec pro ochranu osobních údajů je odpovědný za zajištění celkového dodržování GDPR pro veškeré činnosti v oblasti zpracování osobních údajů [název organizace].

# Účel pracovního místa

Usilovat o dodržování obecného nařízení EU o ochraně osobních údajů (GDPR) a zajistit trvalý soulad s nařízením ve všech klíčových činnostech organizace.

# Zařazení v organizační struktuře

Pověřenec pro ochranu osobních údajů referuje přímo [představenstvu / generálnímu řediteli / vrcholovému vedení].

Pro zajištění nezávislosti pověřence pro ochranu osobních údajů, nesmí být při provádění základních úkolů uvedených v následující části nesmí být žádným způsobem odmítnut nebo penalizován.

Aby se zabránilo jakémukoli případnému střetu zájmů, pověřenec pro ochranu osobních údajů nemůže zastávat ve společnosti žádnou pracovní pozici, které by vedla ke konfliktu zájmů ve smyslu určení účelu a prostředků zpracování osobních údajů.

# Vymezení odpovědností

Pověřenec pro ochranu osobních údajů musí mít odborné znalosti a zkušenosti o právech a postupech v oblasti ochrany osobních údajů, stejně jako další odborné znalosti v oblasti IT, managementu a bezpečnosti, aby zajistil, že organizace splní požadavky nařízení GDPR a příslušné zákony a předpisy o ochraně osobních údajů.

Při referování přímo [představenstvu / generálnímu řediteli / vrcholovému vedení]musí pověřenec pro ochranu osobních údajů informovat a dávat doporučení o ochraně osobních údajů v organizaci v souladu s GDPR a příslušnými právními normami ČR.

Pověřenec pro ochranu osobních údajů zajišťuje, aby byly zásady i postupy zpracování a ochrany byly průběžně aktualizovány, pravidelně se prováděly [plány / kontroly / audity zpracování údajů] a sledovaly hlavní činnosti organizace k zajištění souladu s nařízením GDPR a příslušnými právními normami ČR.

Pověřenec pro ochranu osobních údajů spolupracuje se všemi zaměstnanci ve věcech ochrany osobních údajů.



## Základní úkoly

Pověřenec pro ochranu osobních údajů plní základní úkoly vycházející z požadavků GDPR:

* **Monitorování souladu** s Obecným nařízením (GDPR) a právními normami ČR k problematice zpracování a ochrany osobních údajů a podávat o tomto zprávy [správnímu orgánu / generálnímu řediteli / vrcholovému vedení] organizace.
* Realizace **úkolů spojených s prováděním posouzení** **vlivu**, a to zejména vydání posudku:
  + zda je nebo není nutné provést posouzení vlivu,
  + jakou metodiku při zpracování posouzení vlivu použít,
  + zda posouzení vlivu zpracovat vlastními silami nebo jeho zpracování zadat externě,
  + jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů,
  + zda posouzení vlivu bylo zpracováno správně a zda jeho závěry (ať už vedou či ne k pokračování zpracovatelské operace a bez ohledu na to, jaká ochranná opatření určují uplatnit) jsou v souladu s GDPR;
* **Spolupracovat s dozorovým úřadem (ÚOOÚ) a být styčným bodem pro tento úřad** v otázkách souvisejících se zpracováním osobních údajů a v případě potřeby konzultovat s dozorovým orgánem veškeré další osobní údaje a data.
* Prosazovat **přístup založený na riziku,** a to zejména stanovovat priority pro zajištění ochrany zpracování osobních údajů s vysokým rizikem pro práva a svobody subjektů údajů.
* Zdokumentovat a dále udržovat **přehledy operací zpracování na základě informací od různých oddělení jejich organizace, zodpovědných za zpracování osobních údajů,** a to včetně **vedení jejich registru (evidence).**

## **Další možné pracovní úkoly**

* Informovat a radit organizaci, jejím relevantním partnerům a dodavatelům v ochraně osobních údajů a souladu s nařízením GDPR a zákony o ochraně osobních údajů;
* Informovat a radit všem zaměstnancům v jejich povinnostech při dodržování GDPR a zákonů členských států při nakládání s osobními údaji;
* Spolupracovat při vytvoření systému ochrany osobních údajů (možné i jako součást kybernetické bezpečnosti a zajištění bezpečnosti informací) a pravidelně (1x ročně) tento systém hodnotit.
* Přispívat k rozvoji a udržování všech zásad, postupů a procesů ochrany osobních údajů týkajících se organizace, pokud jde o ochranu a bezpečnost dat;
* Interně zajistit přidělení odpovědností tak, aby došlo k podpoření trvalého souladu s nařízením GDPR a příslušnými právními normami ČR;
* Zajistit možnost školení a povědomí tak, aby byly všichni zaměstnanci, kteří se zabývají operacemi zpracování týkajících se osobních údajů, seznámeni s povinnostmi a požadavky plynoucími z nařízení GDPR a souvisejících zákonů;
* Sledovat dodržování zásad zpracování a ochrany osobních údajů v rámci organizace a doporučovat postupy k zajištění jejich efektivní ochrany;
* Radit v přidělení odpovědnosti za zabezpečení informací;
* Vypracovat/radit při vypracování/ formálních postupů hlášení incidentů GDPR a vyšetřování;
* Radit při zpracování a průběžně sledovat ochranu záznamů zpracování;
* Zjišťovat, do jaké míry jsou osobní údaje shromažďovány, uchovávány a/nebo používány v organizaci a zda jsou řádně kontrolovány a chráněny před ztrátou důvěrnosti, integrity nebo dostupnosti z jakékoli příčiny;
* Revidovat a zhodnotit spolehlivost, přiměřenost a uplatňování bezpečnostních a dalších zásad pro ochranu osobních údajů;
* Identifikovat a otestovat zásady a případně navrhnout další postupy a pravidla, které mohou být zavedeny k zachování důvěrnosti, integrity a dostupnosti osobních údajů.
* Upozornit [správní radu / generálního ředitele / vrcholový management] na případné skutečnosti, které jsou považovány za potenciální rizikové faktory pro řádné zabezpečení osobních údajů v rámci organizace.

# Autorita

Pověřenec pro ochranu osobních údajů má oprávnění k přístupu ke všem systémům organizace, které se týkají shromažďování, zpracování a uchovávání osobních údajů za účelem posouzení užívání a zabezpečení osobních údajů.

Pověřenec pro ochranu osobních údajů má právo očekávat spolupráci všech zaměstnanců při plnění těchto povinností, včetně přístupu k systémům a záznamům. V případě, že nedojde ke spolupráci, pověřenec pro ochranu osobních údajů podá zprávu [správní radě / generálnímu řediteli (CEO) / vrcholnému vedení].

# Platnost a správa dokumentů

Tento dokument je platný od [datum].

Vlastníkem tohoto dokumentu je [pracovní pozice], který musí nejméně jednou ročně zkontrolovat a případně tento dokument aktualizovat.

[pracovní pozice]

[jméno a příjmení]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[podpis]